



Recommendation from the caBIG DSIC – Regulatory SIG
for
caBIG Community-Wide Principles
of
Security, Access-Control, and Confidentiality Administration (caBIG/SA)

Created: 12/20/2004

Version 0.1

**caBIG**cancer Biomedical
Informatics Grid

Although collaborative data-sharing is the goal of caBIG, access to some data expected to be available on or via the caBIG will have to be controlled to ensure that security and privacy needs are met. Thus, security and privacy-related issues must be at the core of the caBIG data generation and access principles, planning and processes. The caBIG DSIC – Regulatory SIG recommends that the entire caBIG community adopt the following principles which we refer to by the shorthand description: *Security Administration (caBIG/SA)*. A common set of caBIG security administration (caBIG/SA) tools and services should be developed as part of the overall caBIG architecture. The common tools and services must be designed to satisfy all of the various privacy, ownership and security needs across the caBIG environment (e.g., patient privacy, regulatory compliance, intellectual property protection, and limited data sharing). Because security requirements for any caBIG resource may change at any time, caBIG/SA tools must be highly flexible, extensible, interoperable, and scalable.

Support for distributed security in a grid environment is an area of active research and development. No currently available tools completely meet the caBIG/SA requirements, and for the indefinite future, all such tools will be undergoing rapid improvement, refinement, and change. Therefore, caBIG/SA tools and services must be deployed in a pluggable, interoperable component manner. That is, caBIG systems should be designed and implemented in a way that allows for the future caBIG system-wide replacement of one or more caBIG/SA tools or services by an improved or new module with little or no change required in the software using the caBIG/SA tools, except to replace one module with another.

The caBIG DSIC Working Group recommends that the caBIG Strategic Planning Working Group and the caBIG Architecture Workspace ensure that *all* caBIG development work (whether done by NCICB, by contractors, or by caBIG participant sites) be done in a manner that results in a uniform, consistent approach to SA across all caBIG systems and resources. Specifically:

- caBIG/SA support should be embedded in the caBIG architecture as a set of basic, generic tools that can be used to meet caBIG/SA requirements at all caBIG sites. caBIG/SA security tools will control access to data sets, while caBIG/SA privacy tools will be integrated with the caBIG Vocabulary and Common Data Element infrastructure as well as assist with de-identification required for grid publication.
- the caBIG community will actually be a community of communities. Therefore, it is important that the caBIG/SA tools and services be implemented specifically to accommodate the union set of needs that will occur across multiple communities with complex relationships.

**caBIG***cancer Biomedical
Informatics Grid*

- caBIG/SA tools and services should be designed at a sufficient level of abstraction so that different security problems do not require different security tools. The same generic security tools should be used for all caBIG needs, with differing use cases accommodated by differences in caBIG/SA access and parameter settings, not by differences in software deployed.
- all caBIG information resources should be required to deploy the full set of caBIG/SA tools. Differences in security requirements across caBIG sites should be reflected in differences in caBIG/SA access and parameter settings, not in differences in software deployed.
- easy to use decision tree structures should be built and made available whenever possible to assist caBIG data generators in determining appropriate levels of privacy, security and access based on the content of their proposed data deposits.

The caBIG DSIC Working Group recommends that the caBIG community adopt the following principles as a general policy:

All caBIG resources and services must be designed, deployed, and operated with the ability to satisfy present and future security requirements. To this end, the caBIG project must develop (or procure) and provide a generic set of caBIG/SA tools and services, along with standard guidelines regarding the use of caBIG/SA systems. These central caBIG/SA tools and services should be available to all caBIG participants who will generate or access data. Use of, or demonstrable compatibility with, these tools and services should be a compliance requirement for anyone who desires to share or use information in the caBIG network.